1. An apparatus for authorized remote access to a target system, the apparatus comprising:

a security module configured to selectively generate an encrypted key in response to a first password and establish a remote communication connection between a remote system and a target system in response to a third password; and

an authorization module configured to decrypt the encrypted key and determine the third password in response to authenticating a second password and identifying a remote user within an authorized user list.

2. The apparatus of claim 1, wherein the first password determines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

3. The apparatus of claim 1, wherein the third password is operable for only a selected period of time.

4. The apparatus of claim 1, wherein the authorization module is configured to communicate with a remote user connected over a secure communication link with the authorization module, and the authorization module is physically remote from the security module.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST 100 SOUTH, SUITE 450
SALT LAKE CITY, UTAH 84101

5. The apparatus of claim 1, wherein a remote user is conditionally added to the authorized user list upon completion of a remote application process.

6. The apparatus of claim 1, further comprising an update module configured to compare the authorized user list to a master list of personnel potentially authorized for remote access to the target system and to selectively remove remote users from the authorized user list not found on the master list.

7. The apparatus of claim 1, wherein the security module and authorization module comprise a log module configured to log actions of the remote user communicating with the target system and the authorization module.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST 100 SOUTH, SUITE 450
SALT LAKE CITY, UTAH 84101

8. An apparatus for authorized remote access to a target system, the apparatus comprising:

a login module configured to establish communications with a remote user in response to a personal password;

a confirmation module configured to determine whether the remote user is identified within an authorized user list;

a decryption module configured to decrypt an encrypted key provided by the remote user in response to identification of the remote user within the authorized user list, the encrypted key sent to the remote user by a target system in response to an access level password;

a password module configured to derive a temporary password from a decrypted version of the encrypted key.

9. The apparatus of claim 8, wherein the access level password defines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

10. The apparatus of claim 8, wherein the temporary password is operable for a selected period of time.

11. The apparatus of claim 8, wherein the authorization module is configured to communicate with a remote user connected remotely to the apparatus over a secure communication link.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST 100 SOUTH, SUITE 450
SALT LAKE CITY, UTAH 84101

12. The apparatus of claim 8, wherein an authorized remote user is conditionally added to the authorized user list in response to approval from at least two supervisors of the user upon completion of a remote application process.

13. The apparatus of claim 8, further comprising an update module configured to compare the authorized user list to a master list of personnel potentially authorized for remote access to the target system and to selectively remove remote users from the authorized user list not found on the master list.

14. The apparatus of claim 8, further comprising a log module configured to log communications between the remote user and the apparatus.

15. A system for authorized remote access to a target system, comprising:

a target system configured to selectively generate an encrypted key in response to a first password and establish a remote communication connection with a remote system in response to a third password;

an authorization server remote from the target system, the authorization server configured to decrypt the encrypted key and determine the third password in response to authenticating a second password and identifying a remote user within an authorized user list, the authorization server configured to then send the third password to the remote system.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST 100 SOUTH, SUITE 450
SALT LAKE CITY, UTAH 84101

16. The system of claim 15, wherein the first password determines a set of commands available to a remote user remotely accessing the target system.

17. The system of claim 15, wherein the third password is operable for a limited time period.

18. The system of claim 15, wherein an authorized remote user associated with the second password is conditionally added to the authorized user list upon completion of a remote application process.

19. The system of claim 15, further comprising an update module configured to compare the authorized user list to a master list of personnel potentially authorized for remote access to the target system and to selectively remove remote users from the authorized user list not found on the master list.

20. The system of claim 15, wherein the target system and authorization server are configured to log actions of a user of the remote system.

21. The system of claim 15, wherein the target system comprises a data storage system.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST 100 SOUTH, SUITE 450
SALT LAKE CITY, UTAH 84101

22. A method for authorized remote access to a target system, comprising:

retrieving an encrypted key from a target system accessed by way of a first password;

connecting to an authorization module using a second password I order to retrieve a third password associated with the encrypted key, the authorization module selectively decrypting the encrypted key in response to determining that a remote user is identified within an authorized user list; and

logging into the target system using the third password.

23. The method of claim 22, wherein the first password determines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

24. The method of claim 22, wherein the third password is operable for a limited time period.

25. The method of claim 22, wherein the remote user communicates over a secure communication link to the authorization module that is physically remote from the target system.

26. The method of claim 22, further comprising completing a remote access application process that conditionally adds a user to the authorized user list.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST 100 SOUTH, SUITE 450
SALT LAKE CITY, UTAH 84101

27. The method of claim 22, further comprising comparing the authorized user list to a master list of personnel potentially authorized for remote access to the target system and selectively removing remote users from the authorized user list not found on the master list.

28. The method of claim 22, further comprising logging actions of the remote user communicating with the target system and the authorization module.

29. A method for authorized remote access to a target system, comprising:

sending an encrypted key to a remote system in response to authenticating a remote user using a first password;

connecting the remote user in response to the user entering a third password associated with the encrypted key, the third password provided to the remote user logged into an authorization module using a second password, the authorization module selectively decrypting the encrypted key in response to determining that the remote user is identified within an authorized user list.

30. The method of claim 29, wherein the first password determines a set of commands available to the remote user logged into a target system, the commands organized according to a plurality of hierarchical access levels.

31. The method of claim 29, wherein the third password is operable for a limited time period.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST BROADWAY, SUITE 450
SALT LAKE CITY, UTAH 84101

32. The method of claim 29, further comprising completing a remote access application process that conditionally adds a user to the authorized user list.

33. The method of claim 29, further comprising comparing the authorized user list to a master list of personnel potentially authorized for remote access to the target system and selectively removing remote users from the authorized user list not found on the master list.

34. The method of claim 29, further comprising logging actions of the remote user communicating with the authorization module and a target system.

35. An apparatus for authorized remote access to a target system, comprising:

means for retrieving an encrypted key from a target system accessed by way of a first password;

means for connecting to an authorization module using a second password to retrieve a third password associated with the encrypted key, the authorization module selectively decrypting the encrypted key in response to determining that a remote user is identified within an authorized user list; and

means for logging into the target system using the third password.

36. The apparatus of claim 35, wherein the first password determines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST 100 SOUTH, SUITE 450
SALT LAKE CITY, UTAH 84101

37. The apparatus of claim 35, further comprising means for logging actions of the remote user communicating with the target system and the authorization module.

38. An article of manufacture comprising a program storage medium readable by a processor and embodying one or more instructions executable by a processor to perform a method for authorized remote access to a target system, the method comprising:

retrieving an encrypted key from a target system accessed by way of a first password;

connecting to an authorization module using a second password to retrieve a third password associated with the encrypted key, the authorization module selectively decrypting the encrypted key in response to determining that a remote user is identified within an authorized user list; and

logging into the target system using the third password

39. The article of manufacture of claim 38, wherein the first password determines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

40. The article of manufacture of claim 38, further comprising logging actions of the remote user communicating with the target system and the authorization module.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
10 WEST 100 SOUTH, SUITE 450
SALT LAKE CITY, UTAH 84101